COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction establishes procedures for individuals to use networked computer systems and other resources of the Pope AFB Wide Area Network (WAN). This instruction applies to all Pope AFB organizations and personnel connected to or receiving services from the Pope AFB WAN. **Records Disposition:** Documentation created by this publication will be maintained and disposed of IAW AFMAN 37-123, *Management of Records* and AFMAN 37-139, *Records Disposition Schedule.*

SUMMARY OF REVISIONS

This publication has been substantially revised and must be reviewed in its entirety.

1. Responsibilities.

1.1. The Pope Network Control Center (NCC) is responsible for supporting Air Force Command, Control, Communications, and Computer (C4) networks utilized in critical DoD and Air Force wartime, business and C4 processes. The NCC is the single focal point on Pope AFB to provide network management and customer support for these services.

1.2. Individual users have the responsibility of properly managing their workstations and other network resources. When personnel log on to their desktop computer systems, they become part of the network and are subject to restrictions. By use of the networked computer, each user consents to monitoring of all activities that take place on that particular computer. Proper use of the network allows access to a variety of services; improper use can adversely affect everyone.

1.3. All requests for local area network (LAN) connection to the existing WAN, or upgrade to an existing LAN, must be documented on AF Form 3215, **C4 Systems Requirement Document**, and submitted to 43CS/SCB through 43 CS/SCX for evaluation and implementation. Changes to the LAN cannot be made without an approved AF Form 3215.

2. Definition. The wide area network (also referred to as the "network") consists of various hardware and software components interacting to provide file, print, e-mail, and other services to users. The network includes individual desktop computers once logged on to the system.

3. Configuration of Networked Computer Systems. Configuration of hardware and software for networked computer systems will be established by the NCC. No modifications to the system configuration are permitted EXCEPT for approved troubleshooting by appointed Functional Systems Administrators, Workgroup Administrators, or NCC personnel. Anyone who makes unauthorized modifications may be subject to disciplinary actions.

4. Network Resource Management. To prevent critical slowdowns, bottlenecks, and other problems that affect the network, all users must prudently manage their files and e-mail to help reduce the amount of disk space and computer resources used. The following standard practices are actions all users should take while using their network workstations.

   4.1. Routine user procedures:

      4.1.1. Delete or save old e-mail files to your local hard drive.

      4.1.2. Delete or save files stored on servers to your local hard drive.

      4.1.3. Use MS Exchange public folders or space on a local server for files you want multiple users to have access to on a frequent basis. Do not use public folders on the Exchange server for routine storage. Review those common access items at least every 14 days and delete files when no longer needed.

      4.1.4. Immediately save e-mail attachments to your hard drive when you get them; then delete the e-mail.

   4.2. Practices to AVOID:

      4.2.1. Do not send e-mail with multiple or large attachments to numerous users (fewer than five is a good guideline.) Instead, send an e-mail message without an attachment to let other users know where to find your file (MS Exchange public folders or organizational folders on a local server.)

      4.2.2. Do not use the file servers for routine storage. Save files to your local hard drive.

   4.3. All "Deleted Item" folders for users who store their mail on the Exchange server should be purged (every day), likewise if you wish to save "Sent Items" they should be moved to your hard drive within 1 day.

5. Password Policy. Each user is responsible for observing the basic criteria of good password management: password composition and length, periodic change, ownership, distribution, entry and safeguarding. Users violating this policy endanger everyone's data and may be denied access to network resources.

   5.1. Password creation guidelines include but are not limited to:

      5.1.1. Passwords must be at least 8 characters long.

      5.1.2. Use a combination of case letters, numbers, and special characters.

      5.1.3. Mix upper and lower case letters.

      5.1.4. Do not use words in dictionaries, slang words, names, or profanity.

5.1.5. Do not use passwords associated with you personally: birth date, dog's name, license plates etc.

5.1.6. Bad examples: last name spelled backwards, "Airf0rce" (hackers often substitute "1" and "0" for "I" and "o". "Airborne", "North Carolina" "Pope AFB", "Password", and the names of children are the most commonly used passwords on Pope AFB.

5.2. Basic protection guidelines:

5.2.1. Protect every computer account with a password.

5.2.2. Change passwords every 90 days or whenever prompted by login.

5.2.3. Guard passwords against compromise.

5.2.4. Do not write passwords down. Do not store them on sticky notes or desk pads near your workstation.

5.2.5. Do not share passwords or allow others to use your login/password.

5.2.6. Change passwords you suspect have been compromised and report the possible compromise to your system administrator.

5.2.7. Do not leave your workstation or terminal unprotected. You are responsible for anything that happens under your user-id. Password protected screen savers are useful for short periods of time, however, they do not provide long term protection. Systems should not be left unattended for extended periods of time (e.g. overnight.)

5.3. You can find out more about passwords in AFMAN 33-23, *Identification and Authentication*

6. Official Use of the Network. Official use includes routine Air Force communications, emergency communications, and communications that the Air Force determines are necessary in the interest of the Federal Government. Official use of e-mail and the Internet includes:

6.1. Conducting official business at work, home, or TDY.

6.2. Answering duty-related e-mail.

6.3. Compiling notes during officially sanctioned conferences or seminars.

6.4. Preparing/reviewing briefings.

6.5. Morale and welfare communications for deployed personnel, when approved by the theater commander.

7. Personal Use of the Network and Internet Access. The agency designee (the first person in the concerned individual's chain of command who is a commissioned military officer or civilian above GS/GM-11) may authorize personal (non-official) use if the following guidelines are met:

7.1. There is no adverse affect on duty performance or the mission of the 43d Airlift Wing.

7.2. The duration and frequency are reasonable and normally during non-duty hours.

7.3. A public interest is being served such as keeping employees at their work stations, educating them on the use of new technology, improving their morale, or enhancing their technical or professional skills.

7.4. There is no adverse reflection on the US Government.

7.5. There is no overburdening of the communications system.

7.6. There is no additional cost to the DoD.

8. E-mail. E-mail is intended to allow military personnel and DoD civilians to expediently send and receive official information locally and worldwide. Improper use of e-mail can greatly hinder the speed and reliability of our electronic mail capability. All e-mail transmissions are routed through a single point within the NCC; therefore, unauthorized transmissions can cause the system to slow down, delaying transmission and receipt of vital information. Inappropriate use of e-mail includes the following:

8.1. Using e-mail to circumvent or bypass the normal chain of command for official actions.

8.2. Illegal, fraudulent, or malicious activities.

8.3. Humorous excerpts from publications.

8.4. Conducting prohibited political or religious activities.

8.5. Any activities for personal or commercial financial gain including for sale items, solicitation of business or services, and chain letters.

8.6. Giving official e-mail addresses to unauthorized personnel, companies or corporations.

8.7. Joining or belonging to groups in an official capacity to include releasing e-mail addresses for solicitation or advertisement from such groups.

9. Screen Savers. Personalized screen savers or wallpaper are authorized if they meet generally accepted ethical standards and are not otherwise prohibited by other applicable regulations. The NCC or base visual information services will not develop, maintain, or accept responsibility for such personalized files.

10. Downloading Software. The Air Force forbids the use of software acquired directly from non-DoD electronic bulletin boards, the public domain, or shareware sources. This software may contain hidden defects that can result in system failure or loss of data. The Air Force allows the use of such software only after it is certified by a software testing facility, such as the Air Force Information Warfare Center (AFIWC), Kelly AFB TX; The major command (MAJCOM) SCTC, or the Standard Systems Center (SSC/SSM) 85 Hodges Avenue South, Maxwell AFB - Gunter Annex AL 36114-6343.

11. Backup of Data Files. All users are responsible for backing up their own critical files, whether those files are stored on their local workstations or organization server. Server backups by the NCC are only for major network recoveries (to include mail servers) and should not be relied upon to protect user data files.

12. Misuse and Unauthorized use of the Network. Incidents involving misuse or unauthorized use of the network may result in administrative, non-judicial or judicial punishment under the UCMJ and the Joint Ethics Regulation, section 3-305. Such incidents may also be a violation of:

AFI 33-129	*Transmission of Information via the Internet*
AFI 33-119	*Electronic Mail (E-Mail) Management and Use*
AFI 33-114	*Software Management*
18 USC Section 641	*Misuse of Public Resources*
18 USC Sections 1029 and 1030	*Computer Fraud and Related Activities*

13. Information about the Network. Direct questions concerning the proper use of networked worksta-tions to the NCC.

FRANK J. KISNER, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

18 USC Section 641, *Misuse of Public Resources*

18 USC Sections 1029 and 1030, *Computer Fraud and Related Activities*

AFI 33-114, *Software Management*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information via the Internet*

AFMAN 33-223*, Identification and Authentication*

Abbreviations and Acronyms

AFB—Air Force Base

AFIWC—Air Force Information Warfare Center

AFSSI—Air Force Special Security Instruction

AL—Alabama

C4—Command, Control, Communications, and Computer

CS—Communications Squadron

DoD—Department of Defense

LAN—Local Area Network

MAJCOM—Major Command

MS—Microsoft

NCC—Network Control Center

SCB—Information Systems Flight

SCX—Plans/Implementation Flight

SSC—Standard Systems Center

TDY—Temporary Duty

TX—Texas

US—United States

WAN—Wide Area Network